Social Networking Security

Adam C. Champion and Dong Xuan
CSE 4471: Information Security

Based on material from H. Townsend (Kansas State U.), G. Bahadur et al. [1], NSA, and U.S. Dept. of State.
Outline

• Overview of Online Social Networking
• Threats and Attacks
• Defense Measures
Online Social Networking (OSN)

• Online Web services enabling people to connect with each other, share information
  – Common friends, interests, personal info, …
  – Post photos, videos, etc. for others to see
  – Communicate via email, instant message, etc.

• Major OSN services: Facebook, Twitter, MySpace, LinkedIn, etc.
“MySpace is a place for friends.”

“MySpace is Your Space.”

“MySpace keeps you connected.”
“Giving people the power to share and make the world more open and connected.”
“Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick frequent answers to one simple question:

What are you doing?”
Your professional network of trusted contacts gives you an advantage in your career, and is one of your most valuable assets. LinkedIn exists to help you make better use of your professional network and help the people you trust in return.”
Delicious is a Social Bookmarking service, which means you can save all your bookmarks online, share them with other people, and see what other people are bookmarking.”
OSN Popularity

• Over 900 million Facebook users worldwide [6]
  – Over 150 million in U.S. [5]
  – Over 450 million access via mobile [6]
  – 300 million pictures uploaded to Facebook daily [6]
• Over 140 million Twitter users; over 340 million Tweets sent daily [7]
• Over 175 million LinkedIn members in over 200 countries [8]
Benefits of OSN Communication

- Vast majority of college students use OSNs
  - Organizations want to market products, services, etc. to this demographic
  - OSNs can help them reach these potential buyers

- OSNs provide communal forum for expression (self, group, mass), collaboration, etc.
  - Connect with old friends, find new friends and connect
  - Play games with friends, e.g., Mafia Wars, Scrabulous
  - Commerce in “virtual items”

- But using OSNs poses security issues for orgs as well as individuals
Outline

• Overview of Online Social Networking
• Threats and Attacks
• Defense Measures
OSN Security Threats/Attacks

• Malware distribution
• Cyber harassment, stalking, etc.
• Information “shelf life” in cyberspace
• Privacy issues:
  – Information about person posted by him/herself, others
  – Information about people collected by OSNs
• Information posted on OSNs impacts unemployment, insurance, etc.
• Organizations’ concerns: brand, laws, regulations
OSN Malware Distribution

• Best-known example: Koobface [9–10]
  – Worm masquerading as Adobe Flash Player update
  – Starting in 2009, OSN users enticed to watch “funny video”, then conned into “updating” Flash
  – Koobface connected infected computers to botnet, served machines ads for fake antivirus software
  – Estimated 400,000–800,000 bots in 2010
  – Facebook outed gang behind Koobface in Jan. 2012, bot server shut down

• Other third-party apps on OSNs like Facebook may contain malware (if not vetted)

• Not to mention hoaxes, “chain letters,” and other cons
OSN 3rd Party Applications

• Games, quizzes, “cute” stuff
• Untested by Facebook – anyone can write one…
• No Terms and Conditions – either allow or deny
• Installation gives developers rights to look at your profile and overrides your privacy settings!

There’s a sucker born every minute.
–P.T. Barnum
OSN Stalking, Harassment, etc.

• Bullies, stalkers, etc. harass people via OSNs
  – High-profile example: Megan Meier’s suicide [11–12]
    • 13-year old Meier killed herself after chatting on MySpace with a 16-year-old boy who made degrading remarks
    • The “boy” was a fake account set up by Lori Drew, mother of Meier’s ex-friend
    • Drew found guilty of violating Computer Fraud and Abuse Act in 2008; acquitted in 2009
    • Most U.S. states have since criminalized cyber harassment, stalking, etc.
  – OSNs (and their members) have played similar roles in mistreating people
OSN Information “Shelf Life”

• Common sense: it’s very difficult to delete information after it’s been posted online

• Indiscreet information can adversely affect college admissions, employment, insurance, etc. [5]

• Twitter gave its entire archive to Library of Congress in 2010 [13]

Originally posted in [2].
OSN Information Privacy (1)

• Information posted on OSNs is generally public
  – Unless you set privacy settings appropriately
  – “I’ll be on vacation” post plus geolocation invites burglars, i.e., “Please Rob Me” [14]

• Indiscreet posts can lead to nasty consequences

Source: [14]

Map from [14]; other images public domain
OSN Information Privacy (2)

• Employers, insurers, college admissions officers, et al. already screen applicants using OSNs
• Recent report from Novarica, research consultancy for finance and insurance industries:

“We can now collect information on buying behaviors, geospatial and location information, social media and Internet usage, and more...Our electronic trails have been digitized, formatted, standardized, analyzed and modeled, and are up for sale. As intimidating as this may sound to the individual, it is a great opportunity for businesses to use this data.” (quoted in [5])
OSN Information Privacy (3)

• Posts that got people fired: [15–16]
  – Connor Riley: “Cisco just offered me a job! Now I have to weigh the utility of a [big] paycheck against the daily commute to San Jose and hating the work.”
  
  – Tania Dickinson: compared her job at New Zealand development agency to “expensive paperweight”

  – Virgin Atlantic flight attendants who mentioned engines replaced 4 times/year, cabins with cockroaches
OSN Information Privacy (4)

- OSNs don’t exactly safeguard posted info…

Facebook

**Facebook and Other Social Media Networks Found Sending Data to Advertisers**

21. MAY, 2010  4 COMMENTS AUTHOR: TIM ROENICKE

works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof. You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.”
URL Shorteners

- bit.ly, TinyUrl, ReadThisURL, NotLong
- Hides the true destination URL – hard to tell where you’re going until you click!

http://www.evil.com/badsite?%20infect-your-pc.html

is now

Organizations and OSNs (1)

• Organizations subject to attacks via OSNs
  – Defamation, damage to org. brand, ™
  – Unauthorized people posting on behalf of org.
  – Negative media coverage, reputation damage

• Case study: BP oil spill fallout [1]
  – Summer 2010: Deepwater Horizon spill (87 days)
  – BP’s public relations didn’t cover OSNs well
  – Angry citizens post on OSNs (@BPglobalPR had 179,000 followers)
  – BP logo “remixed” as oil spill; negative press coverage
Organizations and OSNs (2)

Source: [17]
Organizations and OSNs (3)

• Orgs. have to comply with laws, regulations that OSNs complicate [1]
  – FERPA, HIPAA, Sarbanes-Oxley, etc.
  – Protecting children’s privacy online (due care)

• Ethical issues abound: [1]
  – Should faculty “friend” students?
  – Should a boss “friend” his/her employees?
Outline

• Overview of Online Social Networking
• Threats and Attacks
• **Defense Measures**
Personal Defense Measures (1)

• “Common sense” measures: [1]
  – Use strong, unique passwords
  – Provide minimal personal information: avoid entering birthdate, address, etc.
  – Review privacy settings, set them to “maximum privacy”
    • “Friends of friends” includes far more people than “friends only”
  – Exercise discretion about posted material:
    • Pictures, videos, etc.
    • Opinions on controversial issues
    • Anything involving coworkers, bosses, classmates, professors
    • Anything related to employer (unless authorized to do so)
  – Be wary of 3rd party apps, ads, etc. (P.T. Barnum’s quote)
  – Supervise children’s OSN activity
Personal Defense Measures (2)

• More advice [1]:
  – “If it sounds too good to be true, it probably is”
  – Use browser security tools for protection:
    • Anti-phishing filters (IE, Firefox)
    • Web of Trust (crowdsourced website trust)
    • AdBlock/NoScript/Do Not Track Plus
  – Personal reputation management:
    • Search for yourself online, look at the results…
    • Google Alerts: emails sent daily to you about results for any search query (free), e.g., your name
  – Extreme cases:
    • Cease using OSNs, delete accounts
    • Contact law enforcement re. relentless online harassment
Sick of Facebook’s lack of respect for your data? Add your name and commit to quit!

**Why are we quitting?**

For us it comes down to two things: fair choices and best intentions. In our view, Facebook doesn’t do a good job in either department. Facebook gives you choices about how to manage your data, but they aren’t fair choices, and while the onus is on the individual to manage these choices, Facebook makes it damn difficult for the average user to understand or manage this. We also don’t think Facebook has much respect for you or your data, especially in the context of the future.

For a lot of people, quitting Facebook revolves around privacy. This is a legitimate concern, but we also think the privacy issue is just the symptom of a larger set of issues. The cumulative effects of what Facebook does now will not play out well in the future, and we care deeply about the future of the web as an open, safe and human place. We just can’t see Facebook’s current direction being aligned with any positive future for the web, so we’re leaving.

**What should I know?**

Quitting Facebook isn’t easy. Facebook is engaging, enjoyable and quite frankly, addictive. Quitting something like
Dealing with Shortened URLs

• Many 3rd party online services “un-shorten” URLs:
  – unshorten.me
  – unshorten.it
  – ...

• Some services have browser extensions
• Can unshorten URLs using cURL [18], [19]
  – Idea: follow “Location:” HTTP headers
• Common sense: think before you click
Organizational Defense Measures (1)

• Organizational defense is more complicated:
  – Monitoring employees’ use of OSNs
  – Monitoring org’s name, logo appearance on OSNs
  – Responding to attacks on org. in a timely manner
• Encompasses all parts of an org., not just IT dept!
• This usually entails: [1]
  – Crafting social media policy, disseminating to employees
  – Hiring/training staff to manage org. presence on OSNs
    (with management oversight)
  – Monitoring and reporting employee use of social media
  – …
Organizational Defense Measures (2)

- One defense approach: the HUMOR matrix [1]

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>Human Resources provide companywide policies, procedures, and guidance on acceptable employee use of authorized social media tools. These guidelines and policies provide the correct processes for utilization of social media in all areas of the company, including Marketing and Information Technology.</td>
</tr>
<tr>
<td>Utilization (of Resources and Assets)</td>
<td>Utilization defines the capabilities of secure social media tactics and how these tactics are implemented across technologies and policies to protect a company’s resources and assets.</td>
</tr>
<tr>
<td>Monetary (Considerations)</td>
<td>The monetary resources dedicated to creating a social media strategy and tactics as well as a security strategy have to be aligned to best serve the company.</td>
</tr>
<tr>
<td>Operations (Management)</td>
<td>Operations management is the day-to-day processes that must be followed to implement a security framework, from a technology perspective, as well as from an ongoing maintenance perspective. The objective is to ensure that social media is handled securely as technologies and social media platforms change.</td>
</tr>
<tr>
<td>Reputation (Management)</td>
<td>When all interaction scenarios with social media are calculated, the company’s reputation ultimately benefits. Reputation management is the result of good or bad implementations of social media strategies as well as tactical decisions and provides a monitoring and reporting function that helps to maintain an acceptable level of security and policies over time.</td>
</tr>
</tbody>
</table>

Source: [1], Table 1.1
Organizational Defense Measures (3)

• The HUMOR matrix specifies social media security outcomes, tracks org.’s current status and performance goals over time [1]
  – Outcomes can include employee training regimen, level of employee monitoring, protection of org.’s IP, etc.

• Feedback loop: org. takes action to reach goals, assesses progress periodically (e.g., every 6 mo.)
Organizational Defense Measures (4)

• Example tools: [1], [20]
  – Google Alerts (emails as “search query” appears online)
  – HowSociable (shows mention of org. name/brand on OSNs)
  – SocialGO (create your org.’s own social network)
  – Tech//404 Data Loss Calculator (self-explanatory)
  – Chartbeat (monitor customer engagement on website)
  – EventTracker (monitors employee activity)
  – Many more…
Thank You

Questions & Comments?
References (1)


References (2)

17. https://twitter.com/BPglobalPR